M. ANDERSON BERRY (SBN 262879)
GREGORY HAROUTUNIAN (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

LOWELL PARKER, an individual on behalf of himself and all others similarly situated, Plaintiff, v. METROMILE, INC., Defendant.	Case No.: 3:21-cv-07676 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Lowell Parker ("Plaintiff") brings this Class Action Complaint against Defendant Metromile, Inc. ("Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Metromile is an insurance company. Defendant sells pay-per-mile automobile insurance and licenses its technology to other insurance companies.

2. On or about March 5, 2021, Defendant began notifying customers and state Attorneys General about a data breach that occurred between July 2020 and January 2021 (the "Data Breach").[1] Hackers obtained information from Defendant including the personally identifiable information ("PII") of over one hundred thousand consumers, including, but not limited to, their driver's license numbers.[2] In Metromile's recent Form 8-K filing with the U.S. Securities and Exchange Commission ("SEC"), it admitted:

> Metromile discovered a cybersecurity incident arising out of a software bug related to its online pre-filled quote form and application process. Based on its initial investigation, Metromile determined that unknown persons exploited the software bug to obtain person information of certain individuals, including individuals' driver's license numbers of certain individuals[.][3]

3. Not only did hackers discover Metromile's inadequate safeguards and exploit this "bug" to steal the PII of Plaintiff and Class Members, but, criminals have already used the PII to attempt to steal certain of Plaintiff's and Class Members' identities. This stolen PII has great value to hackers. Because of Defendant's Data Breach, consumers' PII is still available and may be for sale on the dark web for criminals to access and abuse. Consumers who interacted with Defendant face a present and increased, lifetime risk of identity theft.

4. Plaintiff's and Class Members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and their failure to protect the PII.

5. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect consumers' PII, (ii) warn its customers, potential customers, and other consumers of their inadequate information security practices, and (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

6. Plaintiff and similarly situated individuals have suffered injury as a result of

---

[1] https://oag.ca.gov/system/files/Consumer%20Notice%20Letter.pdf (last visited Sept. 28, 2021).

[2] https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/Security-Breach-July2021.pdf (last visited Sept. 28, 2021).

[3] https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (last visited Sept. 28, 2021).

Defendant's conduct. These injuries include: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

7. Plaintiff Lowell Parker is a citizen of New York, residing in the County of Rockland, New York. Mr. Parker received the Notice of Data Breach from Defendants dated March 5, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "security incident that affected your personal information," and that Mr. Parker's "personal information" (including, but not limited to, his name and driver's license number) was involved.

8. Defendant Metromile, Inc. ("Metromile") is a Delaware corporation with its principal place of business at 425 Market Street, Suite 700, San Francisco CA 94105. Metromile, Inc. is an insurance technology company that specializes in pay-per-mile car insurance and insurance automation services. According to its website, Metromile is licensed to sell insurance in eight states.[4] In Metromile, Inc.'s recent SEC Form 8-K filing, it admitted that Metromile, Inc. "determined that unknown persons exploited the software bug [related to Metromile, Inc's "online pre-filled quote form and application process"] to obtain personal information of certain individuals," including Plaintiff and the Class.

III. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or

[4] https://www.metromile.com/ (last visited Sept. 28, 2021).

value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Plaintiff is a New York Resident.

10. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business within this District.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

IV. FACTUAL ALLEGATIONS

Background

12. Defendant is a growing specialized insurer, servicing approximately 95,000 policies and licensed to sell insurance in eight states, including California.[5]

13. In the ordinary course of doing business with Defendant, customers and prospective customers are required to provide Defendant with sensitive PII such as:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number;
- Date of birth;
- Email address;
- Gender;
- Marital status;
- Vehicle information; and
- Other driver information.

[5] https://ir.metromile.com/static-files/e0fb0740-efd2-4591-865c-6a88a24abb5a (last visited Sept. 28, 2021).

14. Defendant collects this information about prospective customers to provide insurance coverage and quotes for car insurance.

15. Defendant promises to provide confidentiality and security for personal information, including by promulgating and placing privacy policies on its website. For example, Defendant states: "Metromile is committed to protecting your information from unauthorized access and disclosure. We have certain physical, electronic, and procedural safeguards in place that are designed to help protect the security and integrity of your information both during transmission and once it is received."[6]

The Data Breach

16. On or about March 5, 2021, Defendant began notifying consumers and state Attorneys General about a data security incident that occurred for several months starting in July of 2020 and lasting through January 2021.

17. According to the Notice of Data Breach letters and letters sent to state Attorneys General, Metromile, "learned that unknown bad actors identified an unlawful way to use our online quote form and application process to obtain some individuals' personal information."[7]

18. According to the Notice, Defendant, "took steps to address this incident promptly and thoroughly" with their investigation concluding in January of 2021. [8]

19. However, despite first learning of the Data Breach in January 2021 and concluding the investigation soon thereafter, Defendant did not take any measures to notify affected Class Members until March 5, 2021.

20. Moreover, Defendant did not provide detail to consumers about what information was compromised. For example, Plaintiff Parker was informed that, "your information, including your driver's license number," was compromised in the data breach. But the true scope of what personal information belonging to Plaintiff was stolen due to Metromile's "bug" is still unclear.

---

[6] https://www.metromile.com/privacy/ (last visited Sept. 28, 2021).

[7] https://oag.ca.gov/system/files/Consumer%20Notice%20Letter.pdf (last visited Sept. 28, 2021).

[8] *Id*.

Defendant Was Aware of the Risks of a Data Breach

21. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members and the general public to keep their PII confidential and to protect it from unauthorized access and disclosure.

22. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

23. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the breach.

24. Data breaches, including those perpetrated against the banking/credit/financial sector of the economy, have become widespread. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in breaches involving the banking/credit/financial sector. [9]

25. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

26. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. [10] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud. [11]

---

[9] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Sept. 28, 2021).

[10] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Sept. 28, 2021).

[11] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying

27. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

28. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and members of the Class, including Social Security numbers, driver's license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

29. Plaintiff and members of the Class now currently face years of constant surveillance and monitoring of their financial and personal records and loss of rights. The Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

30. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and members of the Class.

Defendant Failed to Comply with FTC Guidelines

31. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

32. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

---

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

33. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

34. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

35. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

36. Defendant was at all times fully aware of their obligation to protect the PII of the consumers they interact with. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Failed to Comply with Industry Standards

37. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

38. Best cybersecurity practices that are standard in the financial services industry

include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

39. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

40. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the Data Breach.

The Value of PII to Cyber Criminals

41. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth, driver's license numbers, and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

42. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12]

43. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited Sept. 28, 2021).

for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

44. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

45. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

46. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old

[13] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 28, 2021).

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Sept. 28, 2021).

number anymore.

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[15]

47. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach is a dream for hackers and a nightmare for Plaintiff and the Class. The stolen personal data of Plaintiff and members of the Class represents essentially one-stop shopping for identity thieves.

48. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

49. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

50. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

51. Identity thieves may commit various types of crimes such as immigration fraud,

---

[15] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 28, 2021).

[16] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited Sept. 28, 2021).

obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

52. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Consumers who provided this information to Defendant now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[17]

55. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

56. According to a recent article in the New York Times, cyber thieves are using driver's licenses obtained via insurance company application prefill processes to submit and

[17] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 28, 2021).

fraudulently obtain unemployment benefits.[18] That is exactly what happened to Plaintiff Parker in this case, as detailed below. An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiff's and Class Members' Damages

57. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered two-years of inadequate identity protection credit monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach.

58. Moreover, the monitoring services offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face the risk of identity theft for more than two years, rather it is an ongoing threat of identity theft and financial fraud.

59. Defendant entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

60. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

61. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

62. Plaintiff and Class Members have been, and face substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal activities based on their PII as

[18] *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021) https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Sept. 28, 2021)

potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class members.

63. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

64. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

65. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

66. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

67. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

68. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

69. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Parker's Experience

70. Plaintiff Lowell Parker received the Notice of Data Breach from Defendant Metromile, dated March 5, 2021, on or about that date. The Notice stated that the exposed PII "affected [his] personal information," including but not limited to his full name and driver's license number.

71. As a result of receiving the Data Breach notice, Mr. Parker has spent time dealing with the consequences of the Data Breach, including confirming the legitimacy of the Data Breach, reviewing the information compromised by the Data Breach, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, attempting (multiple times) to sign up for the free credit monitoring service offered by Defendant, signing up for Norton LifeLock identity theft protection (at a cost to him of $100 per year), and freezing his credit with the relevant credit bureaus.

72. Following this Data Breach, on or about March 3, 2021, the New York State Department of Labor ("NYSDOL") notified Mr. Parker that an unauthorized third party filed a "claim for unemployment insurance benefits" using Mr. Parker's PII. Mr. Parker did not apply for these benefits. The letter stated: "We believe that someone, using identity information stolen from you either recently or in the past, attempted to file this claim"; and that: "This is not due to a breach of NYSDOL's systems, but may be the result of prior data breaches of other institutions over time such as banks, insurance companies, your employer, etc."

73. Mr. Parker is not aware of any other data breaches that could have resulted in the theft of his sensitive PII and driver's license number. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

74. Mr. Parker stores any and all documents containing his PII in a safe and secure digital location and destroys any documents he receives in the mail that contain any of his PII or that may contain any information that could otherwise be used to compromise his identity. Moreover, he uses complex passwords for his online accounts for added security, and multi-factor authentication for particularly sensitive account.

75. Mr. Parker suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Defendant did not adequately safeguard and was compromised in and as a result of the Data Breach.

76. Mr. Parker also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

77. Mr. Parker has suffered imminent and impending injury arising from the present and substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

78. Mr. Parker has become worried about this theft of his PII and has a continuing interest in ensuring that Defendant protect and safeguard his PII, which remains in Defendant's possession, from future breaches.

V. CLASS ALLEGATIONS

79. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> **All natural persons residing in the United States whose PII was compromised in the Data Breach announced by Defendant on or about March 5, 2021 (the "Nationwide Class").**

80. The New York Subclass is defined as follows:

> **All natural persons residing in New York whose PII was compromised in the Data Breach announced by Defendant on or about March 5, 2021 (the "New York Class").**

81. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

82. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

83. **Numerosity**: The Class is so numerous that joinder of all members is impracticable.

Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

84. **Commonality**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

a. When Defendant actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiff and members of the Class;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiff and members of the Class;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep the PII of Plaintiff and members of the Class secure and to prevent loss or misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused damage to Plaintiff and members of the Class;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Class that their PII had been compromised; and

j. Whether Plaintiff and the other members of the Class are entitled to credit monitoring and other monetary relief.

85. **Typicality**: Plaintiff's claims are typical of those of the other members of the Class because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

86. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

87. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

88. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole.

89. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Class to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

90. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 89.

91. Defendant owed a duty to Plaintiff and Nationwide Class Members to exercise reasonable care in obtaining, using, and/or protecting their PII from unauthorized third parties.

92. The legal duties owed by Defendant to Plaintiff and Nationwide Class Members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Nationwide Class Members in its possession;

b. To protect PII of Plaintiff and Nationwide Class Members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Nationwide Class Members of the Data Breach.

93. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

94. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Nationwide Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

95. Defendant breached their duties to Plaintiff and Nationwide Class Members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

96. Defendant knew or should have known that their security practices did not adequately safeguard Plaintiff's and Nationwide Class Members' PII.

97. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and those of the Nationwide Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Nationwide Class Members' PII during the period it was within Defendant's possession and control.

98. Defendant admits that it "discovered a cybersecurity incident arising out of a software bug related to its online pre-filled quote form and application process. Based on its initial investigation, Metromile determined that unknown persons exploited the software bug to obtain personal information of certain individuals, including individuals' driver's license numbers[.]"

99. Defendant breached the duties it owed to Plaintiff and Nationwide Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach to detect and prevent a breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to consumers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

100. Due to Defendant's conduct, Plaintiff and Nationwide Class Members are entitled to comprehensive identity monitoring and credit monitoring. Identity and credit monitoring is reasonable here because the PII taken can be used for identity theft and other types of financial fraud against Plaintiff and the Nationwide Class Members.

101. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

102. As a result of Defendant's negligence, Plaintiff and Nationwide Class Members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Nationwide Class Members, including ongoing credit monitoring.

103. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the Nationwide Class Members suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class)

104. Plaintiff and Class members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 89.

105. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

106. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Nationwide Class due to the valuable nature of the PII at issue in this case.

107. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

108. Plaintiff and members of the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

109. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Nationwide Class.

110. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity

addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of consumers in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Nationwide Class.

111. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

112. Plaintiff and Class members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 89.

113. When Plaintiff and Nationwide Class Members provided their PII to Defendant in exchange for Defendant's products, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their PII.

114. Defendant solicited and invited Plaintiff and Nationwide Class Members to provide their PII as part of Defendant's regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiff and Nationwide Class Members on one hand, and Defendant on the other hand. Plaintiff

and Nationwide Class Members accepted Defendant's offers by providing their PII to Defendant in connection with their purchases from Defendant.

115. When entering into these implied contracts, Plaintiff and Nationwide Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

116. Defendant's implied promise to safeguard Plaintiff's and Nationwide Class Members' PII is evidenced by a duty to protect and safeguard PII that Defendant required Plaintiff and Nationwide Class Members to provide as a condition of entering into consumer transactions with Defendant.

117. Plaintiff and Nationwide Class Members paid money to Defendant to purchase products or services from Defendant. Plaintiff and Nationwide Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

118. Plaintiff and Nationwide Class Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from customers' continued use of Defendant's insurance services—that Defendant would adequately safeguard PII. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Nationwide Class Members.

119. Plaintiff and Nationwide Class Members value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

120. Plaintiff and Nationwide Class Members fully performed their obligations under their implied contracts with Defendant.

121. Defendant breached their implied contracts with Plaintiff and Nationwide Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

122. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Nationwide Class Members sustained damages as alleged herein.

123. Plaintiff and Nationwide Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

124. Plaintiff and Nationwide Class Members also are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Nationwide Class Members.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

125. Plaintiff and Class members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 89.

126. Defendant owes duties of care to Plaintiff and Nationwide Class Members which require them to adequately secure their PII.

127. Defendant still possess Plaintiff's and Nationwide Class Members' PII.

128. Defendant does not specify in the *Notice of Data Breach* letter what steps they have taken to prevent this from occurring again.

129. Plaintiff and Nationwide Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

130. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests,

and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Nationwide Class Members for a period of ten years; and

h. Meaningfully educating Plaintiff and Nationwide Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

131. Plaintiff and Class members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 89.

132. Defendant benefited from receiving Plaintiff's and Nationwide Class Members' PII by their ability to retain and use that information for their own benefit. Defendant understood this benefit.

133. Defendant also understood and appreciated that Plaintiff's and Nationwide Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

134. Plaintiff and Nationwide Class Members who were customers of Defendant conferred a monetary benefit upon Defendant in the form of monies paid for services available from Defendant.

135. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Nationwide Class Members. Defendant also benefited from the receipt of Plaintiff's and Nationwide Class Members' PII, as Defendant used it to facilitate the transfer of information and payments between the parties.

136. The monies that Plaintiff and Nationwide Class Members paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

137. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

138. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed Plaintiff and Nationwide Class Members that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, their shareholders, and their consumers.

139. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Nationwide Class Members. Defendant continue to benefit and profit from their retention and use of the PII while its value to Plaintiff and Nationwide Class Members has been diminished.

140. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiff's

and Nationwide Class Members' PII, while at the same time failing to maintain that information secured from intrusion and theft by hackers and identity thieves.

141. As a result of Defendant's conduct, Plaintiff and Nationwide Class Members suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and Nationwide Class Members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

142. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Nationwide Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Nationwide Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

143. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Nationwide Class Members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

COUNT VI
Violation of New York GBL § 349
(On Behalf of Plaintiff and the New York Class)

144. Plaintiff and New York Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 89.

145. Defendant violated New York's General Business Law § 349(a) when it engaged in deceptive, unfair, and unlawful trade, acts, or practices in conducting trade or commerce and through furnishing of services, including but not limited to:

a. Misrepresenting material facts to Plaintiff and the New York Class by stating it would maintain adequate security measures to protect from unauthorized disclosure the PII belonging to Plaintiff and the New York Class;

b. Misrepresenting material facts to Plaintiff and the New York Class by representing itself as a business that would comply with state and federal laws pertaining to the privacy and security of PII belonging to Plaintiff and the New York Class;

c. Omitting and/or concealed material facts regarding its inadequate privacy and security protections for PII belonging to Plaintiff and the New York Class;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain sufficient privacy and security related to PII belonging to Plaintiff and the New York Class resulting in a data breach, which is in violation of duties imposed on Defendant by state and federal laws, including the Federal Trade Commission Act (15 U.S.C. § 45);

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff and the New York class in a timely and accurate manner, which violates duties imposed on Defendant by New York General Business Law § 899-aa(2).

146. Defendant knew, or should have known, that its computer systems and security practices were inadequate to protect PII entrusted to Defendant by Plaintiff and the New York Class. Further, Defendant knew, or should have known, that the risk of theft of PII through a data breach was highly probable.

147. Defendant was in a superior position to know the true facts regarding its deficient data security and should have disclosed this fact to the Plaintiff and New York Class.

148. Defendant mislead consumers regarding the security of their network and ability to secure PII it collected by failing to disclose the true facts regarding their deficient data security. This constitutes false and misleading representation, which had the capability, tendency, and impact of deceiving or misleading consumers, such as Plaintiff and the New York Class.

149. Defendant's representations were material representations, which consumers such as Plaintiff and the New York Class relied upon to their detriment.

150. Defendant's conduct is unconscionable, deceptive, and unfair, and is substantially likely to and did mislead consumers such as Plaintiff and the New York Class acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and the New York class have been injured because they were not timely notified of the Data Breach causing their PII to be compromised.

a. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff and the New York Class had their PII disclosed to unauthorized third parties, which caused damage to Plaintiff and the New York Class.

b. Plaintiff and the New York class seek relief under New York General Business Law § 349(h), including actual damages, statutory damages, treble damages, injunctive relief, and/or attorney's fees, expenses, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the New York Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data

collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs

sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 30, 2021

Respectfully Submitted,

By: */s/ M. Anderson Berry*
M. ANDERSON BERRY

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiff and the Proposed Class